International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:1, No:6, 2007

Net-Banking System as a Game

N. Ghoualmi-Zine, and A. Araar

***Abstract*—**In this article we propose to model Net-banking system by game theory. We adopt extensive game to model our web application. We present the model in term of players and strategy. We present UML diagram related the protocol game.

***Keywords*—**Game theory, model, state, web application.

I. Introduction

GAME theory is a branch of mathematics that studies the interactions of multiple independent decision makers that try to fulfill their own objectives. Today, it is applied to telecommunications as the users try to ensure the best possible quality of service. In recent years, game theoretic research on ad hoc networking has emerged. Game theory is a set of analytical developed to study situation in which self-interested parties interact with each other according to rules. Thus, it makes possible to model a wider range of real life situations.

The distance visualization with different interfaces knows an important evolution. The interfaces permit to access to data of type text and images. Several domains see an expansion of using the web like e-commerce, e-business, e-learning… Net banking application is one of more important web application. These transfer systems require a security system which protects these data during their transfer, because for raisons of confidentiality.

Exchanged information is very important and should be organized. We have to define who sends, who receives. Also, we have to define constraints for each participant. Therefore we have to offer to users (bank and client) fair, reliable and rational exchange information on the different types of networks. Game theory is adequate to model Net-Banking system. Article contains an introduction as section 1. Section 2 gives background in theory game. Section 3 presents extensive game. Section 4 presents Net baking system modeled as game. Section 5 presents UML diagrams related to game model. A conclusion finishes the article.

II. Theory Game Background

Game theory is a set of analytical developed to study situation in which self-interested parties interact with each other according to rules. Since these kinds of situations occur in, exchange protocols game theory is very appropriate. Parties of a given exchange protocol find themselves as a game. Game is called the protocol game. The protocol parties are modeled as players. The protocol itself is represented as a set of strategies (one strategy for each protocol party).

Games can be classified into different categories according to their properties. We present below a brief classification [1].

- Non cooperative and cooperative games
- Strategic and extensive games
- Zero-sum games
- Games with perfect and imperfect information
- Games with complete and incomplete information

III. Extensive Games

Extensive games eliminate the limitation of the simultaneous decisions, thus they make possible to model a wider range of real life situations. Thus, we present below a formal presentation and protocol game [2].

A Formal Presentation

Next, we formulate an extensive game based on [2]. It should be noted that for simplicity the following formulation does not allow simultaneous actions of the players, i.e. the game has perfect information. An extensive game with imperfect information can be formulated similarly. In the strategic and extensive games, the solution of a game is a set of actions or strategies that will result in Nash equilibrium.

- A set N (the set of players).
- A set H of sequences (finite or infinite) of actions that satisfies the following three properties.
  - The empty sequence θ; is a member of H.
  - If $\left(a^k\right)_{k=1\ldots K}$ $K \in H$ (where K may be infinite) and L < K then $\left(a^k\right)_{k=1\ldots L} \in$ H.
  - If an infinite sequence $\left(a^k\right)_{k=1}^{\infty}$ satisfies H for every positive integer L then $\left(a^k\right)_{k=1}^{\infty} \in$ H.

(Each member of H is a history; each component of a history is an action taken by a player.) A history $\left(a^k\right)_{k=1\ldots K} \in$ H is terminal if it is infinite or if there is no $\left(a^{k+1}\right)$ such that $\left(a^k\right)_{k=1\ldots K+1} \in$ H. The set of terminal histories are denoted Z.

- A function P that assigns to each non terminal history (each member of H\Z) a member of N. (P is the

N. Ghoualmi-Zine is with the Computer Sciences Department, Badji Mokhtar University Annaba, 23000, Algeria (e-mail: ghoualmi@yahoo.fr).
A. Araar is with the Faculty of Computer Sciences, University of Ajman, UAE (e-mail: araar@ajman.ac.ae).

player function, P(h) being the player who takes an action after the history h.)

- For each player $i \in$ N a utility function U_i on Z.

B. Protocol games

The protocol game of an exchange protocol is intended to model all the possible interactions of the (potentially misbehaving) protocol parties. The correct behavior of each party is represented by a particular strategy within the protocol game.

We should note that we consider only two-party exchange protocols (i.e., protocols that involve only two main parties and possibly a trusted third party) because most of the exchange protocols proposed in the literature are two-party exchange protocols.

IV. Net-Banking as Game

We assume that the network that is used by the protocol participants to communicate with each other is reliable, which means that it delivers messages to their intended destinations within a constant time interval. Such a network allows the protocol participants to interact in a synchronous fashion. We will model this by assuming that the protocol participants interact with each other in *rounds*, where each round consists of the following two phases [3]:

1. each participant generates some messages based on her current state, and sends them to some other participants;
2. each participant receives the messages that were sent to her in the current round, and performs a state transition based on her current state and the received messages.

A. Players in Net-Banking System

We model each protocol participant (i.e., the two main parties) as player. In addition, we model the communication network as a player too. Therefore, the player set P of the protocol game is defined as $P = (p_1, p_2, p_3, net)$ where $p1$ and $p2$ represent the two main parties of the protocol, $p3$ stands for the trusted third party, and *net* denotes the network. If the protocol does not use a trusted third party, then $p3$ is omitted. We denote the set $P \setminus \{net\}$ by P'.

Therefore, main players in Net-banking are costumer which represents client and account that represents bank's server denoted by P'. We assume that network is reliable by cryptographic systems. We shall present in next section a cryptographic method.

B. Information sets in Net-banking

We define two types of events: send and receive events. The send event snd (m; j) is generated for player $i \in P'$ when she submits a message $m \in M_\pi$ with intended destination $j \in P'$ to the network, and the receive event rcv (m) is generated for player $i \in P'$ when the network delivers a message $m \in M_\pi$ to i. We denote the set of all events by E.

The local state $\sum_i(q)$ of player $i \in P'$ after action sequence q is defined as a tuple $\langle \alpha_i(q), H_i(q), r_i(q) \rangle$ where:

- $\langle \alpha_i(q) \rangle \in$ {true; false} is a Boolean, which is true iff player i is still active after action sequence q (i.e., she did not quit the protocol);
- $\langle H_i(q) \rangle \subseteq E \times N$ is player i's local history after action sequence q, which contains the events that were generated for i together with the round number of their generation;
- $\langle r_i(q) \rangle \in N$ is a non-negative integer that represents the round numbers for player i after action sequence q.

Initially, we have: $\langle \alpha_i(q) \rangle$ = true, $\langle H_i(q) \rangle = \phi$, and $\langle r_i(q) \rangle$ = 1 for every player $i \in P'$.

C. Protocol Game in Net-Banking system

In previous work we presented Syverson's protocol as protocol game that guaranties integrity, authentication, no-repudiation and confidentiality [4]. To secure exchange in Net-Banking system we had proposed to mix cipher methods: cipher at character level and at bit level. At Character level we use θ- Vigenere that we developed in previous work [3]. At bit level we use standards cipher like AES, DES, etc. We introduce θ- Vigenere in Syverson's protocol because encryption key is random and encryption system is symmetric. Syverson's protocol has to transmit the triple, which represents key in θ-Vigenere. So the receipt is allowed to decrypt message at character level. The application consists to encrypt at character level by θ- Vigenere cipher and with random K at bit level. Where K' is the basic key used by Vigenere cipher and on which message is divided in blocs [5]. Then we obtain: 1- A and B denote the two participants; 2- K_A^{-1}, K_B^{-1} denote their private keys, 3- Item A, item B denote the items that they exchange, 4- dsc A denotes the description of item A, 5- K denotes a randomly chosen secret key, 6- enc is a symmetric-key encryption at bit level, 7- K', θ denotes a randomly chosen key, 8- enc' is symmetric-key encryption at character level where enc'= θ- Vigenere

V. UML Diagrams Related to Game Model

A. The ObjectDiagram

We present below the object diagram[7] that represents player parties (see Fig.1). The object customer represents client party and account represents bank's server party. Transaction is an object that represents history of client. For each transaction between customer and his account we save in transaction class information, which save historic of last ten transactions.

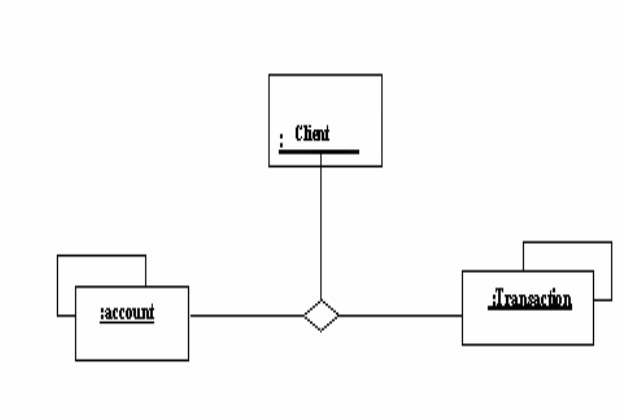
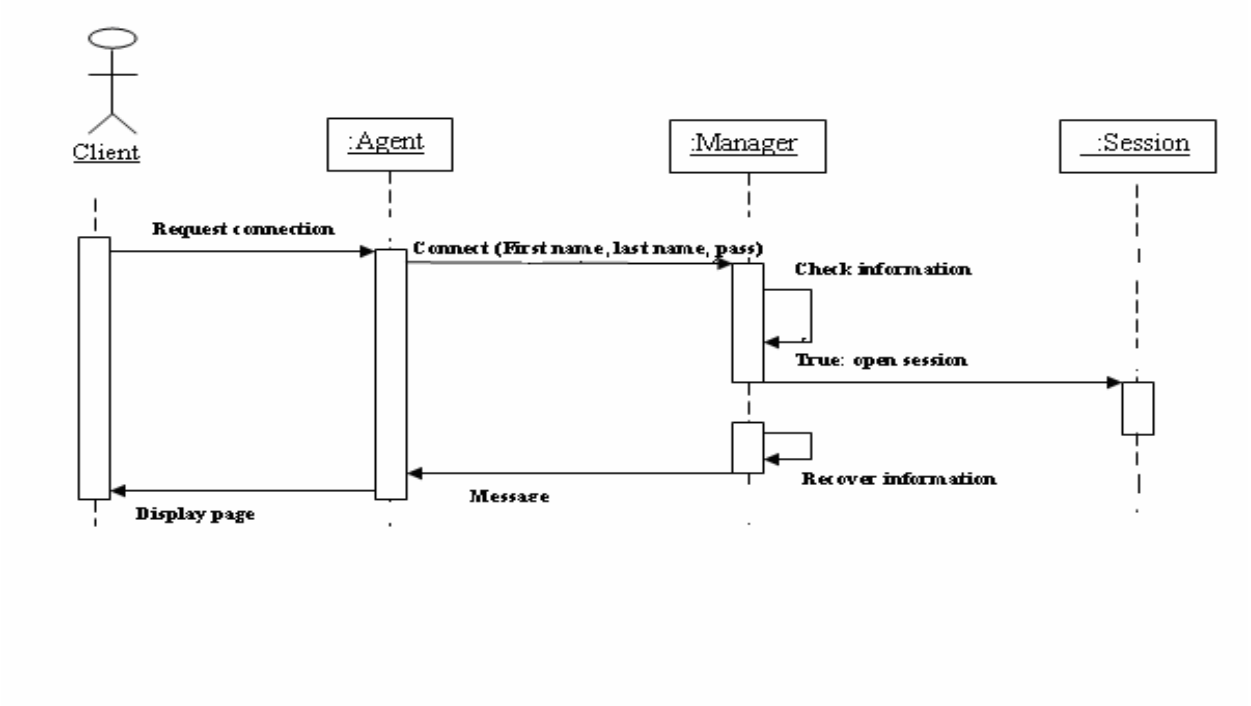


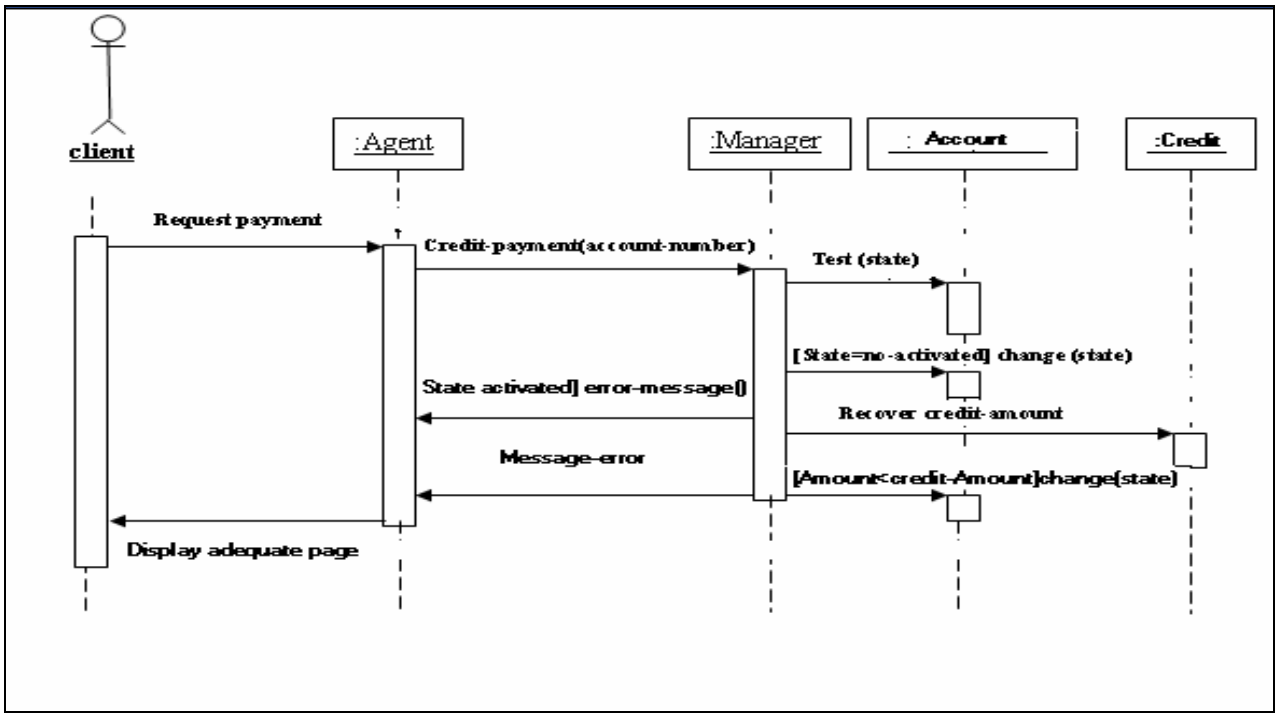
Fig. 1 Object diagram

B. Connection Process Sequence Diagram

Each object in the Net-banking passes by different states through transitions; we study each object apart showing its different states, events provoking transitions of these states.



C. Payment Credit with Activated Account Sequence Diagram



VI. Conclusion

We have developed a Net-banking application because this kind of application is in expansion on the web. We modeled the application as game. Game theory is very adequate for such application. We presented UML Diagram that represents interactions. In Future work we'll develop protocol game as secured exchange protocol.

References

[1] M. J. Osborne and A. Rubinstein. A Course in Game Theory. MIT Press, Cambridge, 1994.

[2] T. Fent, G. Feichtinger, and G. Tragler. *A dynamic game of offending and law enforcement.* International Game Theory Review, 4(1):71–89, 2002.

[3] N. Ghoualmi-Zine & A.Araar, "*Secured Net-Banking by θ-vigenere in Syverson's protocol*", IEEE Catalog Number:05EX949, ISBN 0-7803-8735-X, Library congress:2004110879, AICCSA 2005.

[4] Levente Buttyan, Jean Pierre Hubaux, Srdjan Capkun, '*A formal model of rational exchange and its application to the analysis of Syverson's protocol*', 2003 IOS Press, journal on computer security, 15th IEEE security foundation workshop, 2003.

[5] P. Syverson, '*Weakly secret bit commitment: Applications to lotteries and fair exchange*', In Proceedings of the IEEE computer security foundations workshop, pp. 2-13, 1998.

[6] M. Jakobsson, J.P. Hubaux, and L. Huttyan. *A micropayment scheme encouraging collaboration in multi-hop cellular networks* In Proceedings of Financial Crypto 2003, January 2003.

[7] Conallen J., *Concevoir des applications Web avec UML*,Editions Eyrolles, 2000.